Part No. 210676-Z
May 2003

4655 Great America Parkway
Santa Clara, CA 95054

Release Notes for the Business Policy Switch 2000

Software Version 2.5.2

NORTEL NETWORKS™

Copyright © 2003 Nortel Networks

All rights reserved. May 2003.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks NA Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

BayStack, Business Policy Switch 2000, Nortel Networks, the Nortel Networks logo, and Optivity Policy Services are trademarks of Nortel Networks.

Adobe and Acrobat are trademarks of Adobe Systems Incorporated.

All other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks NA Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks NA Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Introduction

These release notes for the Nortel Networks* Business Policy Switch 2000* software version 2.5.2 provide information about software and operational issues not included in the Business Policy Switch 2000 (BPS 2000) software version 2.5 guides.

To obtain the software version 2.5.2, download the following files from the Nortel Networks customer support web site at http://support.nortelnetworks.com/:

- bps2k252_4.img (software image file—without SSH feature)
- bps2k252s_5.img (software image file—includes SSH feature)
- bps2kdiag_2503.bin (diagnostics image file)

You must download the diagnostics file as well as the software file.

Note: Encryption algorithms included in the SSH feature are subject to export controls under the U.S. Department of Commerce Bureau of Export Administration Act. Nortel Networks is required to take adequate precautions to ensure that software products containing encryption, and made available on a server connected to the internet, are not exported without being subject to some form of verification procedures.

When downloading the image file that includes the SSH feature, you will first be required to fill out a questionnaire verifying that you are eligible to download the software.

Note: If you choose to download and install the image file that includes the SSH feature, you will no longer have access to the console interface on the device.

To obtain the Java* Device Manager (DM) software to manage the BPS 2000, download the following file from the Nortel Networks customer support web site at http://support.nortelnetworks.com/:

- DM 5.5.8—You must upgrade the JRE software, which is on the web site, to version 1.3.0 at this time also.

These release notes provide information on version 2.5.2 and cover the following topics:

- "Upgrading software," next
- "New features and enhancements" on page 8
- "New and enhanced NNCLI commands" on page 10
- "Resolved issues" on page 13
- "Known issues" on page 17
- "Known limitations" on page 22
- "Related publications" on page 24
- "How to get help" on page 25

Upgrading software

Note: Use the Command Line Interface (CLI), console interface (CI) menus, or the Web-based management system to upgrade to software version 2.5.2. For detailed instructions, refer to *Using the Business Policy Switch 2000 Version 2.5*, *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5,* and *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5.*

Note: To prevent configuration corruption of devices in a stack when upgrading to software version 2.5.2, you must disable IGMP snooping.

Different procedures for upgrading must be followed depending on whether a pure BPS 2000 or Hybrid stack is being upgraded.

The stacking software compatibility requirements are as follows:

- Pure BPS 2000 stack—All units must be running the same software version.
- Hybrid stack:
  - — All BPS 2000 units must be running the same software version.
  - — All BayStack 410 units must be running the same software version.

— All BayStack 450 units must be running the same software version.
— All software versions must have the identical ISVN.

This section discusses the following topics:

- "Upgrading software in a Pure BPS 2000 stack," next section
- "Upgrading software in a Hybrid stack" on page 5

Upgrading software in a Pure BPS 2000 stack

To download, or upgrade, software in a Pure BPS 2000 stack:

1. Download the operational software image.
2. Download the diagnostics image.

However, if you are currently using software version 1.0, 1.0.1, or 1.1, you must upgrade to software version 1.1.1 before upgrading to version 2.5.2.

Note: Once you begin the upgrading process, do not interrupt the process at all.

Upgrading software in a Hybrid stack

The physical order of the units and the unit numbering in the Hybrid stack does not affect the upgrading process at all, however you must ensure that a BPS 2000 switch is Unit 1 and is the base unit.

Note: In order to upgrade BayStack 410 and BayStack 450 software in a hybrid stack, the stack must be fully redundant. All cables in the stack must be installed and operating properly. If the cables are not installed properly, the BayStack units will fail to upgrade. A message is displayed on consoles connected to BayStack 410 and BayStack 450 switches:

```
Primload Error - 2009 Switch will reset in 5
seconds...
```

Before you attempt to download new software (or upgrade software) to a Hybrid (mixed) stack, you *must* ensure that the Interoperability Software Version Numbers (ISVN) are identical. That is, the ISVN number for the BayStack 450 switch and BayStack 410 switch must have the same ISVN as the BPS 2000. If the ISVNs are not the same, the stack will not operate. The ISVNs and the accompanying software release are:

- ISVN 1
  - BayStack 410 or Bay Stack 450—version 3.1
  - BPS 2000—versions 1.0 and 1.0.1
- ISVN 2
  - BayStack 410 or BayStack 450—versions 4.0, 4.1 and 4.2
  - BPS 2000—versions 1.1, 1.1.1, 1.2, 2.0, 2.0.5, 2.0.5.20, 2.5, 2.5.1, and 2.5.2

This section describe the steps for the following software upgrades:

- "Upgrading software when ISVN is 2," next section
- "Upgrading software when ISVN is 1" on page 7

Upgrading software when ISVN is 2

To upgrade a Hybrid stack to BPS 2000 software version 2.5.2 when the ISVN numbers of the units are 2:

1. Download the BPS 2000 image file.

   The system resets.

2. Download the BPS 2000 diags file.

   The system resets.

Note: Once you begin the upgrading process, do not interrupt the process at all.

Upgrading software when ISVN is 1

To upgrade a Hybrid stack to BPS 2000 software version 2.5.2 when the ISVN numbers of the units are 1:

1 Download the BPS 2000 image file and the BayStack 450/410 file *simultaneously.*

The system resets.

Note: If you do not download both the BPS 2000 and BayStack 410/450 images simultaneously, the stack may not form.

---

2 Download the BPS 2000 diags file.

The system resets.

3 Validate that the ISVN is 2 on both the BPS 2000 and the BayStack 410/450.

Note: Once you begin the upgrading process, do not interrupt the process at all.

To find out which version of the BPS 2000 software is running, use the Console Interface (CI) menus, the CLI or the Web-based management system:

- CI menus—From the main menu of the Console, choose Systems Characteristics menu. The software currently running is displayed in sysDescr.
- Web-based management system—Open the System Information page, which is under Administration on the main menu. The software currently running is displayed in the sysDescription field.
- CLI—Run the `show sys-info` command, which is in the privExec command mode. The software currently running is displayed in sysDescr.

Refer to Appendix B of the *Using the Business Policy Switch 2000 Software Version 2.5* for complete information on interoperability and compatibility between the BPS 2000 and BayStack switches.

New features and enhancements

There are no new features offered with BPS 2000 software version 2.5.2.

The following new feature is offered with the BPS 2000 software version 2.5.1:

- With software release 2.5.1, the BPS 2000 switch supports Far End Fault Indication (FEFI). When a fiber optic transmission link to a remote link fails, the remote device indicates the failure and the port is disabled. To use FEFI, you must enable autonegotiation on the port.

Note: FEFI does not work with the BPS2000-2GE MDA because the BPS2000-2GE MDA does not support autonegotiation.

The following new features and enhancements are offered with the BPS 2000 software version 2.5:

- Secure Shell—You may now establish a secure shell (SSH) connection to the BPS 2000. The SSH protocol can provide strong authentication and secure communication over an unsecured network. Refer to *Using the Business Policy Switch 2000 Version 2.5*, *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5,* and *Reference for the Business Policy Switch 2000 Management Software Operations Software Version 2.5* for more information about this feature.
- Per VLAN egress tagging—BPS 2000 ports can now be configured to transmit frames tagged on some VLANs, and untagged on other VLANs. Refer to *Using the Business Policy Switch 2000 Version 2.5*, *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5, Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5* and *Reference for the Business Policy Switch 2000 Management Software Operations Software Version 2.5* for more information about the VLAN tagging feature.
- QoS enhancements—There are now up to 24 Layer 2 filters per unit available for configuration and a '% OutOfProfile' column has been added to the QoS Statistics Table. Refer to *Using the Business Policy Switch 2000 Version 2.5*, *Reference for the Business Policy Switch 2000 Command Line Interface*

Software Version 2.5, Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5 and *Reference for the Business Policy Switch 2000 Management Software Operations Software Version 2.5* for more information about the QoS enhancements.

- SNMPv3 commands added to NNCLI—Several new SNMPv3 commands have been added to the command line interface. Refer to *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5* for more information about the new SNMPv3 commands.
- Additional enhancements to the NNCLI—Several commands have been added to the command line interface. Refer to "New and enhanced NNCLI commands" on page 10 for more information about the additional commands.
- System Log enhancement—If a switch does not join a stack because of an improper Stack Operational Mode setting, a message indicating this will be written to the system log of the base unit and to the system log of the improperly configured device.
- System Log enhancement—If a switch does not join a stack because the software version number does not match the software version number of the base unit, a message indicating this will be written to the system log of the base unit and to the system log of the device.
- 128 VLANs per filter are now supported—You can now configure up to 128 VLANs per filter. Refer to *Using the Business Policy Switch 2000 Version 2.5*, *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5, Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5* and *Reference for the Business Policy Switch 2000 Management Software Operations Software Version 2.5* for more information about configuring VLANs.

Additional new security enhancements

In addition to Secure Shell, the following new security enhancements are offered with software release 2.5:

- Access to SNMPv3 MIBs is hidden from SNMPv1 and SNMPv2 access.
- The SNMP read/write community string is hidden if the user is logged in to the web interface as a read-only user.
- The SNMPv3 menu is unavailable when logged in to the web interface as a read-only user.

- The Security menu is unavailable when logged in to the web interface as a read-only user.
- The length of passwords is now hidden when entering passwords in any of the Security menus of the web interface.

New and enhanced NNCLI commands

This section discusses the new and enhanced NNCLI commands included in software version 2.5 that are not described in *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5*. This section covers the following topics:

"show arp-table command," next section

"show autotopology settings command" on page 11

"show autotopology nmm-table command" on page 12

"vlan igmp command" on page 13

show arp-table command

The `show arp-table` command displays the ARP table, showing the IP to MAC address mapping. The syntax for the `show arp-table` command is:

```
show arp-table
```

The `show arp-table` command is in the privExec command mode.

The `show arp-table` command has no parameters or variables. Figure 1 displays a sample output of the `show arp-table` command.

Figure 1 show arp-table command output

```
BPS2000#show arp-table

Port IP Address      MAC Address

---- --------------- -----------------

21   134.177.150.1   00:E0:16:53:85:82

BPS2000#
```

show autotopology settings command

The `show autotopology settings` command displays the current autotopology settings. The syntax for the `show autotopology settings` command is:

```
show autotopology settings
```

The `show autotopology settings` command is in the privExec command mode.

The `show autotopology settings` command has no parameters or variables. Figure 2 displays a sample output of the `show autotopology settings` command.

Figure 2 show autotopology settings command output

```
BPS2000#show autotopology settings

Autotopology:  Enabled

Last NMM Table Change:  6871

Maximum NMM Table Entries:  100

Current NMM Table Entries:  2

BPS2000#
```

show autotopology nmm-table command

The `show autotopology nmm-table` command displays the NMM table. The syntax for the `show autotopology nmm-table` command is:

```
show autotopology nmm-table
```

The `show autotopology nmm-table` command is in the privExec command mode.

The `show autotopology nmm-table` command has no parameters or variables. Figure 3 displays a sample output of the `show autotopology nmm-table` command.

Figure 3 show autotopology nmm-table command output

```
BPS2000#show autotopology nmm-table

Slot Port IP Addr          Seg ID MAC Addr          Chassis Type     BT LS   CS

---- ---- --------------- ------ ----------------- ---------------- -- --- ----

0    0    134.177.150.75  0      00:04:38:D9:97:61 BPS2000          12 Yes HTBT

1    21   134.177.150.180 1550   00:60:FD:EB:47:F4 BayStack 450     12 Yes HTBT

BPS2000#
```

vlan igmp command

The `vlan igmp` command configures IGMP snooping parameters. The syntax for the `vlan igmp` command is:

```
vlan igmp <1-4094> [snooping {enable|disable}]
[proxy {enable|disable}] [robust-value <value>]
[query-interval <time>] [v1-members {add|remove} <portlist>]
[v2-members {add|remove} <portlist>]
```

The `vlan igmp` command is in the config mode.

Table 1 describes the parameters and variables for the `vlan igmp` command.

Table 1 vlan igmp command parameters and variables

Parameters and variables	Description
<1-4094>	Enter the VLAN to configure for IGMP.
snooping {enable|disable}	Enables or disables the VLAN for IGMP snooping.
proxy {enable|disable}	Enables or disables the VLAN for IGMP proxy.
robust-value <value>	Enter the robust value you want for IGMP.
query-interval <time>	Enter the number of seconds you want for the query interval of IGMP.
v1-members <portlist>	Enter the list of ports for port membership for IGMP v1.
v2-members <portlist>	Enter the list of ports for port membership for IGMP v2.
add|delete	Specifies if the ports are to be added or removed. If this parameter is omitted, ports are added.

Resolved issues

The following issue was resolved in version 2.5.2:

- Stack resets with IGMP joins/leaves no longer cause configuration corruption of other units in the stack. (CR Q00664743)

The following issues were resolved in version 2.5:

- Topology packets are now sent out on all DMLT trunks. (CR Q00481670)
- CLI `show` commands issued concurrently from multiple telnet sessions will now display properly. (CR Q00544734)
- The switch will now properly respond to PC management stations with valid IP addresses ending in .255 or .0. Also, the switch can now ping devices with valid IP addresses ending in .255 or .0. (CR Q00079077, Q00524724 and Q00536687)
- 450-1 GBIC MDAs in a hybrid stack are now display correctly via the base unit console. (CR Q00541493)
- When upgrading from software version 1.1.x to 2.x.x, QoS configuration settings will remain intact. (CR Q00511186)
- The error message `% No such VLAN` is now displayed if you try to delete a non-existent VLAN using the CLI. (CR Q00526098)
- Link LED on BPS 2000 MDAs properly turns off when link is disconnected. (CR Q00305369)
- You are prevented from changing the management VLAN to a VLAN with no members.
- Downloading the binary configuration file to the switch will now properly set AuthenticationTrap and Autotopology settings to the expected state. (CR Q00153286)
- When configuring QoS metering, you are prevented from setting the committed burst size smaller than the token fill rate.
- MIB object s5ChasVer now correctly returns the BayStack 410. (CR Q00497983)
- All MAC addresses are now displayed in CAPITAL letters (Hex A through F) in the CLI.
- When configuring QoS metering profiles using the web interface, you are now prevented from creating a profile with the same name as an existing profile. (CR Q00386872)
- The console now correctly refreshes to display the removal or insertion of GBICs.
- MIB object s5AgSysStackIpAddress can now be configured properly using the `set` command. (CR Q00488187)
- The BPS 2000 Image If Newer option added to the software download menu now works correctly in a hybrid stack.

The following issues were resolved in version 2.0.5.20:

- Downloading an ASCII configuration file will no longer result in a broadcast storm on a BPS 2000 switch that is set to DMLT. (CR Q00514963)
- Configuring an MLT link (two ports on the same unit) will no longer cause a loop when the switch is reset. (CR Q00514981)
- In previous releases, in a mixed or pure stack, with IGMP and static router port configured, if multiple VLANs were created and then one VLAN in the middle of the table was deleted at later time, DMLT/MLT trunks did not function correctly. This has been corrected in software release 2.0.5.20.
- IGMP queries are no longer sent to a port that is configured as static router port, received queries are forwarded to ports only if the Unknown Multicast feature is enabled.

The following issues were resolved in version 2.0.5:

- When configuring Port Mirroring on a specified MAC address, resetting the switch no longer causes instabilities in the system. (CR Q00155176)
- When deleting a VLAN member of a Spanning Tree Group (STG), the first port of the MLT is now correctly removed from the STG. (CR Q00316370)
- You no longer need to reboot the BPS 2000 switch when you add a policy where you configure shaping parameters. (CR Q00139108)
- When using Web management on a stack of BPS 2000 switches and accessing the Port Error Summary page, if the page contains more than six entries, the system will no longer hang. (CR Q00170933)
- The command `dot1dStpPortEnable.x` now works properly to disable a port. (CR Q00391212)
- The Redundant Power Supply Unit (RPSU) LED no longer returns the wrong value when using Device Manager. (CR Q00279588)
- You can now log in via the Web interface using RADIUS authentication. (CR Q00416483)
- You can now use the CLI to configure flow control for BPS 2000-2GE ports. (CR Q00415228)
- When autonegotiation is enabled for a Gigabit link, the flow control menu in the Web interface no longer offers the choice of Symmetric or Asymmetric. Flow control is disabled. (CR Q00416485)

- Sixteen character usernames cause RADIUS authentication to fail. Web and console interface now correctly limit usernames to 15 characters for RADIUS authentication. (CR Q00359668)
- The `show port-statistics` command has been added to all command modes. It was previously available only in the interface configuration mode. (CR Q00310716)
- In a Hybrid stack, when a station is moved to a different VLAN, it will properly communicate with the new VLAN (CR Q00384459)
- STP will now be correctly disabled on the monitor port when port mirroring is enabled. (CR Q00415229)
- If the connection is interrupted during the download of the diagnostics code, the switch will not try to use the incomplete diagnostics. (CR Q00417287)
- Timing issues during switch resets have been corrected so that large BPS 2000 stacks will no longer go into a loop when switches are reset. (CR Q00251306)
- The default global filter only applies to Ethernet II encapsulated packets. Default and customer-configured global filters can no longer corrupt IEEE 802.3 or SNAP (Subnetwork Access Protocol) encapsulated packets by modifying the Differentiated Services Code Point (DSCP) of the packets. (CR Q00230928)

Note: You cannot modify the DSCP of IEEE 802.3 or SNAP encapsulated packets.

The following issues were resolved in version 2.0.2.3:

- The allowable ranges for QoS Meter Committed Rate, Max Burst Rate, and Max Burst Duration in the CLI now correctly match the Web-based management ranges. (CR Q00209291)
- Malformed SNMP message packets are now discarded. These packets can no longer cause the SNMP task to crash, disabling SNMP, CLI and Web access. The BPS 2000 will no longer be affected by SNMP vulnerability issues documented on February 12, 2002 by CERT/CC in their SNMP advisory (VU#107186 and VU#854306).

The following issues were resolved in version 2.0:

- The `show log` and `clear log` CLI commands now function correctly. (CR Q00047028)
- The Web-based management system now correctly displays all configured VLANs. (CR Q00101635)
- IGMP Proxy now works correctly on tagged ports with multiple VLANs in multiple spanning tree groups. (CR Q00084861)
- It no longer takes a long time for the ASCII config file with extensive configurations to complete. (CR Q00091334)
- The flash synchronization was every 60 seconds. This synchronization now occurs very 2 minutes and 30 seconds.
- The setting of Learn by Ports in the MAC address-based security no longer changes to disabled after you reset the switch or stack. (CR Q00147573, Q00043550)
- You can now ping the switch if the MAC address-based learning security setting for the management port is set to Enabled. (CR Q0008448)
- The BPS 2000 switch no longer caches RADIUS responses (so that connections were authorized even when server is down). (CR Q00043170)

Known issues

The following issues are known to exist in version 2.5.2 of the BPS 2000 software:

- To prevent configuration corruption of devices in a stack when upgrading to software version 2.5.2, you must disable IGMP snooping.
- You can no longer view statistics in bar graph format in the web interface. *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5* incorrectly states that bar graph charts are available in the web interface.
- In large stacks (four or more units) running large QoS configurations, upgrading from version 2.0.5 to the SSH version of 2.5 may result in the loss of QoS configuration. The workaround is to reset the stack to the default settings, perform the upgrade to version 2.5 and reconfigure your stack as needed.

- Repeatedly running the `show ssh global` command more than 100 times may cause unexpected behavior in the device. (CR Q00562971)
- Pressing Ctrl-N several times while in the System Characteristics page of the console interface may cause unexpected behavior in the device. (CR Q00562295)
- You must reset the stack to default settings before downgrading from 2.5.0.x to 2.0.5.x or 2.0.x. (CR Q00559924)
- When a non-default STG is set to ‘inactive’, any member port that has STP participation state other than ‘disabled’ will never move from the state “listening”. This port will not pass traffic until the STG is configured as ‘active’ or the port’s STP participation state is set to ‘disabled’. To completely disable Spanning Tree on the STG you must set the port STP participation state to ‘disabled’ for all ports belonging to that STP. (CR Q00524691)
- Due to hardware restrictions, when using one-way/bidirectional conversation between port X and port Y, unknown, multicast, and broadcast frames are not mirrored to the monitor port when ports X or Y are in full duplex. (CR Q00510591)
- When you create a policy that references shaping parameters, the 802.1p and Drop Precedence values must be changed either by using the system defaults or explicitly by the action.
- Using the Device Manager, port VLAN membership may be displayed incorrectly on some units in a stack of six or more. (CR Q00567688)
- In a hybrid stack with a large number of VLANs, VLAN port settings made using the CLI interface may not be correctly applied. (CR Q00543617)
- If you try to restart the SSH server via the `ssh` command shortly after stopping it with the `no ssh` command, the action will fail. The workaround is to wait for one minute after shutting down the SSH server before trying to enable it. (CR Q00520055)
- In a hybrid stack with IGMP traffic and proxy enabled, host reports are not consolidated as expected. (CR Q00509844)
- In a hybrid stack, STP for MultiLink Trunking cannot be correctly configured from the console on a BayStack 410/450. The workaround is to connect to a BPS 2000 console in the stack. (CR Q00540982)
- The port configuration menus allow you to set the port speed for the BPS2000-2GT, BPS2000-1GT and BPS2000-2GE ports to 10 Mbps and 100 Mbps, however the port will always operate at 1000 Mbps. The spanning tree cost correctly remains “1” regardless of the port configuration setting. (CR Q00510677)

- In a hybrid stack, when connecting to the console of a BayStack 410/450, BPS 2000 fan status is not reported correctly. (CR Q00498018)
- When using DM to set the COPS Retry Interval in the Retry Setting tab of the COPS dialog box, the RetryIntvl field incorrectly says the value is in seconds. The value is in centi-seconds. Enter the desired number of seconds multiplied by 10 in this field. (CR Q00521950)
- When using MAC security, the Learn by ports field is not correctly updated when units are renumbered. (CR Q00535885)
- Entering a large number of characters at the console start up screen while the stack is forming can cause the units to reset. (CR Q00527637)
- You cannot download the diagnostics image file if you are connected to the console of a non-base unit. You must use the console connected to the base unit or use Telnet or the web interface when downloading the diagnostics image file. (CR Q00525256)
- In a hybrid stack, you can improperly modify MLT without disabling it first when connected to the console of a BayStack 450. Workaround is to connect to a BPS 2000 console in the stack. (CR Q00541707)
- In a hybrid stack, BPS2000-2GT, BPS2000-1GT and BPS2000-2GE MDAs do not appear correctly in the Hardware Unit Information screen when connected to the console of a BayStack 450. The workaround is to connect to a BPS 2000 console in the stack. (CR Q00543265)
- When changes are made to the MAC Address Security list, it is not enabled after the update. The workaround is to disable and re-enable Global Security. (CR Q00530284)
- While a stack is forming, entering the System Log menu on a unit may cause it to reset. The workaround is to wait until the stack has formed before entering the System Log menu. (CR Q00535865)
- When upgrading to 2.5 from 1.x, telnet access will be enabled, even if it was disabled before the upgrade. You must disable telnet access again, after the upgrade. (CR Q00391178)
- When you set a large number of RMON alarms, setting a short sampling interval for each alarm will cause the switch appear to be locked up as all CPU resources will be used to attempt the samples.(CR Q00411371)

  The workaround is to set larger sampling intervals for RMON alarms.
- The QoS shaping feature does not work in a stacked configuration; it works only in a BPS 2000 standalone unit. (CR Q00153202)
- QoS shaping is supported only on IP filters.

- In a hybrid stack, if STP is disabled for a switch, some DMLT ports may show incorrect Spanning Tree participation settings. (CR Q00425777)
- The CPU/Memory Utilization feature is unavailable in version 2.5 (CR Q00169353)
- When you are working with a mixed stack and download the v.2.x software for the BPS 2000 and the v.4.1.x software for the BayStack 450 *simultaneously*, the software may not load on all units.

  The workaround is to download the software separately to the BPS 2000 units and to the BayStack 450 units. The units reset after the software downloads in both cases.
- The flooded packets and filtered packets counters return incorrect results for the BPS 2000-1GT, BPS 2000-2GT, and BPS 2000-2GE MDA (they always display 0). (CR Q00137290)
- Nortel Networks recommends that you do not use MAC Address Security (BaySecure) on any MultiLink Trunk ports.
- When you renumber a stack of pure BPS 2000, check the port mirroring configuration. You may have to manually reconfigure the ports you want for port mirroring. (CR Q00156278)
- ASCII configuration file name maximum string length is 29, rather than 30, characters. (CRQ00107944)
- When you attempt to save the configuration to the TFTP server, it may not work the first time. (CR Q00153972)

  Workaround is to save it a second time, when it definitely saves.
- When you are using the CLI and attempt to set a 10/100 Mbps port to 1000 Mbps, the port mode resets to autonegotiation. (CR Q00153171)
- If you are working with a mixed, or Hybrid, stack and are downgrading the software, the BPS 2000 units will reset to factory default but the BayStack 450 units will not default.

  The workaround is to default the entire stack.
- When you are working with QoS configurations and you delete a filter, that filter will continue to operate until you reset the BPS 2000. (CR Q00071760)
- When working in a mixed stack with BayStack 450 v.4.0/4.1 and BPS 2000, only the BPS 2000 displays the IP address of the stack. (CR Q00079143)

- When using the CLI and entering the IP address and mask in the form of A.B.C.D/<0-32>, you can also enter the values in the form of A.B.C.D/E.F.G.H.
- Occasionally when you have disabled MAC address-based security, the ports will still register as an intrusion. (CR Q00092007, Q00091998)

  The workaround is to reset the stack.

- The port speed and duplex you set using the ASCII configuration file may show incorrectly in the console display that shows port speed and duplex. The actual speed and duplex will be what you set with the configuration file, but the console display for these parameters may be incorrect. (CR Q00083014)

  The workaround is to use the CLI.

- When you are using DM to display the spanning tree group memberships, the port members may not display correctly. (CR Q00093350) Use the console interface (CI) menus, the CLI, or the Web-based management system to double-check the spanning tree group memberships.
- EAP configuration changes made at one console or using DM may not automatically display on other consoles. (CR Q00044484, CR Q00045315)

  The workaround is refresh the console and the correct data displays.

- If you rapidly add and delete VLANs (more than 1 per second) using DM, some of the VLANs may not be configured.

  The workaround is allow a few seconds to elapse between adding and deleting ports and VLANs if you are using DM.

- The ASCII configuration file does not support multiple spanning tree operations. (CR Q00088185)

  Use the CI menus, CLI, the Web-based management system, or DM to configure multiple spanning tree groups.

- The Multicast Group Membership table may display duplicate entries when the switch is in Distributed MultiLink Trunking (D-MLT) mode. However, the trunks function properly; this is a display problem only. (CR 138095-1)
- In a BPS 2000-only stack, the entire stack is reset to default values when you return the base unit to default values. (CR 145501-1)
- To disable a port that is part of a Truck group, use either Device Manager (DM) or the Console Interface (CI) management system menus (you can use the Telnet connection). With the Web-based management system, you may be unable to disable ports that are part of MLTs. (CR 146607-1)

- When the High Speed Flow Control Autonegotiation feature is set to enabled (the default), the port only advertises support for 1000 Mb/s operation, in full-duplex mode. If you experience problems between the Business Policy Switch and other network devices, set Autonegotiation to *disabled* on both sides of the link.
- Gigabit MDA
  - When viewing Active Phy information from the console interface, the console must be connected to the unit containing the Gigabit MDA (the BayStack 450-1SR MDA and the BayStack 450-1LLR MDA) to display the appropriate Phy information. Incorrect information may be displayed if you connect to a unit not containing a Gigabit MDA.
  - When you remove a Gigabit MDA from a switch, the Active Phy of the effected unit displays the new status. However, occasionally, the Active Phys of the other units in the stack or remote units will not display the new status.

Known limitations

The following limitations are known to exist:

- The current usable filters for the BPS are:
  - 200 policies
  - 100 interface groups
  - 200 IP filters and filter groups
  - 24 IP filters with same Source Address (18 nested subnets)
  - up to 24 Layer 2 filters and filter groups
  - 200 meters
  - 128 actions
  - 62 shapers

Note: Each in-profile action, out-of-profile action, and statistics tracking session uses 1 filter each.

- You can configure protocol-based VLANs, with a sum total of "N" PID values not to exceed 14 (Table 2). If you are not running the spanning tree protocol, you have 15 PIDs available.

Table 2 Protocol and PID values

Protocol Name	Number of PID values (N)
Ip Ether2	2
Ipx 802.3	1
Ipx 802.2	1
Ipx Snap	2
Ipx Ether2Snap	2
AplTk Ether2Snap	2
Declat Ether2	1
DecOther Ether 2	10
Sna 802.2	2
Sna Ether2	1
NetBios 802.2	2
Xns Ether2	2
Vines Ether2	1
Ipv6 Ether2	1
Usrdef	1
Rarp Ether2	1

For more information on Predefined Protocol Identifiers (PIDs), hexadecimal values, and associated protocols, refer to *Using the Business Policy Switch 2000 Software Version 2.5*.

Related publications

For more information about the BPS 2000 switch, refer to:

- *Release Notes for the Business Policy Switch 2000 Software Version 2.5* (part number 210676-T)
- *Using the Business Policy Switch 2000 Software Version 2.5* (part number 208700-D)
- *Using Web-Based Management for the Business Policy Switch 2000 Software Version 2.5* (part number 209570-D)
- *Reference for the Business Policy Switch 2000 Management Software Version 2.5* (part number 209322-D)
- *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5* (part number 212160-C)
- *Getting Started with the Business Policy Switch 2000 Management Software* (part number 209321-A)
- *Business Policy Switch 2000 Installation Instructions* (part number 209319-A)
- *Installing Media Dependent Adapters (MDAs)* (part number 302403-H)
- *Installing Gigabit Interface Converters and Small Form Factor Pluggable Interface Converters* (part number 312865-B)
- *Installing Optivity Policy Services* (part number 306972-E Rev 00)
- *Managing Policy Information in Optivity Policy Services* (part number 306969-F Rev 00)
- *Release Notes for Optivity Policy Services Version 2.0* (part number 306975-E Rev 00)
- *Task Map - Installing Optivity Policy Services Product Family* (part number 306976-D Rev 00)
- *Known Anomalies for Optivity Policy Services Version 2.0* (part number 306974-E Rev 00)
- *Using the Optivity Quick2Config 2.2 Client Software* (part number 207810-B)
- *Installing and Administering Optivity Quick2Config 2.2* (part number 207890-B)
- *Configuring Business Policy Switches with Optivity Quick2Config 2.2* (part number 311208-A)

- *Release Notes for Optivity Quick2Config for Business Policy Switch 2000, v.2.2.1* (part number 310621-A)

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat* Reader to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

How to get help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone
Europe, Middle East, and Africa	(33) (4) 92-966-968
North America	(800) 4NORTEL or (800) 466-7835
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

Additional information about the Nortel Networks Technical Solutions Centers is available from at http://www.nortelnetworks.com/help/contact/global/. You can also visit our technical support web site at http://support.nortelnetworks.com/ where you can download software updates and documentation for Nortel Networks products.

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to http://www.nortelnetworks.com/help/contact/erc/.